CLAIMS:

What is claimed is:

1. A method comprising:

operating a first provisioning system authorized to provision a processing device on a network, wherein the provisioning system is within a trusted environment; and

using the first provisioning system to authorize a second provisioning system outside the trusted environment to provision the processing device.

2. A method as recited in claim 1, wherein said using the first provisioning system to authorize a second provisioning system comprises using the first provisioning system to provision authorization of the second provisioning system in the processing device.

3. A method as recited in claim 2, wherein said using the first provisioning system to authorize a second provisioning system comprises using the first provisioning system to send a provisioning message to the processing device, the provisioning message indicating authorization of the second provisioning system to provision the processing device.

4. A method as recited in claim 3, wherein the provisioning message further specifies one or more parameters which the second provisioning system is authorized to provision.

5. A method as recited in claim 1, wherein said using the first provisioning system to authorize a second provisioning system comprises using the first provisioning system to send a provisioning message to the processing device, the provisioning message indicating authorization of a plurality of other provisioning systems, including the second provisioning system, to provision the processing device.

6. A method as recited in claim 5, wherein the provisioning message further specifies one or more parameters which each of the other provisioning systems is authorized to provision.

7. A method as recited in claim 1, wherein the processing device is a mobile device on a wireless network.

8. A method as recited in claim 7, further comprising using a digital signature to provision the mobile device.

9. A method as recited in claim 8, wherein said using a digital signature to provision the mobile device comprises using the digital signature to authenticate the source of the provisioning message.

10. A method as recited in claim 8, further comprising using the first provisioning system to provision the mobile device with a digital certificate identifying the first provisioning system.

11. A method as recited in claim 8, further comprising using the first provisioning system to provision the mobile device with a digital certificate identifying the second provisioning system.

12. A method as recited in claim 11, wherein the second provisioning system is on a second network that is outside the trusted environment and separate from, but coupled to, the wireless network.

13. A method as recited in claim 12, wherein the first provisioning system has unrestricted authorization to provision the mobile device, and the authorization of the second provisioning system to provision the mobile device is regulated from the first provisioning system.

14. A method as recited in claim 8, further comprising using the first provisioning system to provision the mobile device with digital certificates identifying a plurality of other provisioning systems.

15. A method comprising:

operating a primary trusted provisioning domain (TPD); and

using the primary TPD to provision a mobile device on a wireless network by sending a provisioning message to the mobile device, the provisioning message specifying a secondary TPD authorized to provision the mobile device and an identifier of one or more parameters which the secondary TPD is authorized to provision.

16. A method as recited in claim 15, wherein the primary TPD is within a trusted environment, and wherein the secondary TPD is outside the trusted environment.

17. A method as recited in claim 16, wherein the secondary TPD communicates with the mobile device via a second network that is outside the trusted environment.

18. A method as recited in claim 16, further comprising using the primary TPD system to provision the mobile device with a digital certificate identifying the secondary TPD to enable the secondary TPD to provision the mobile device using a digital signature.

19. A method as recited in claim 15, wherein the provisioning message specifies a plurality of secondary TPDs authorized to provision the mobile device and one or more parameters which each of the secondary TPDs is authorized to provision.

20. A method comprising:

operating a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of mobile devices on a wireless network;

using the primary provisioning server to provision a digital certificate of the primary provisioning server in each of the mobile devices;

using the primary provisioning server to provision a digital certificate of a secondary provisioning server in the mobile devices, wherein the secondary provisioning server is on a second network outside the trusted environment; and

using the primary provisioning server to provision the mobile devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the mobile devices.

21. A method as recited in claim 20, wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers.

22. A method as recited in claim 20, further comprising using the primary provisioning server to specify one or more parameters which the secondary provisioning server is authorized to provision in the mobile devices.

23. A method as recited in claim 20, further comprising using the primary provisioning server to provision the mobile devices with information indicating authorization of a plurality of secondary provisioning servers to provision the mobile devices.

24. A method as recited in claim 23, further comprising using the primary provisioning server to specify one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices.

25. A method as recited in claim 24, wherein said using the primary provisioning server to specify one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope.

26. A method as recited in claim 20, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the primary provisioning server.

27. A provisioning system comprising:

a processor;

a data communication device coupled to the processor to communicate data with one or more remote systems; and

a memory coupled to the processor and storing instructions for execution by the processor to cause the provisioning system to provision a mobile device on a wireless network by sending a provisioning message to the mobile device, the provisioning message specifying a second provisioning system authorized to provision the mobile device and an identifier of one or more parameters which the second provisioning system is authorized to provision.

28. A provisioning system as recited in claim 27, wherein said provisioning system is within a trusted environment, and wherein the second provisioning system is outside the trusted environment.

29. A provisioning system as recited in claim 28, wherein the second provisioning system communicates with the mobile device via a second network that is outside the trusted environment.

30. A provisioning system as recited in claim 28, further comprising using said provisioning system to provision the mobile device with a digital certificate identifying the second provisioning system to enable the second provisioning system to provision the mobile device using a digital signature.

31. A provisioning system as recited in claim 27, wherein the provisioning message specifies a plurality of secondary provisioning system authorized to provision the mobile device and one or more parameters which each of the secondary provisioning system is authorized to provision.

32. A machine-readable program storage medium storing instructions which, when executed in a processing system, configure the processing system to operate as a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of mobile devices on a

wireless network, such that the instructions configure the processing system to execute a process comprising:

provisioning a digital certificate of the primary provisioning server in each of the mobile devices;

provisioning a digital certificate of a secondary provisioning server in the mobile devices, wherein the secondary provisioning server operates outside the trusted environment; and

provisioning the mobile devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the mobile devices.

33. A machine-readable program storage medium as recited in claim 32, wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers.

34. A machine-readable program storage medium as recited in claim 32, wherein the process further comprises specifying one or more parameters which the secondary provisioning server is authorized to provision in the mobile devices.

35. A machine-readable program storage medium as recited in claim 32, wherein the process further comprises provisioning the mobile devices with information indicating

authorization of a plurality of secondary provisioning servers to provision the mobile devices.

36. A machine-readable program storage medium as recited in claim 35, wherein the process further comprises specifying one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices.

37. A machine-readable program storage medium as recited in claim 36, wherein said specifying one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope.

38. A machine-readable program storage medium as recited in claim 32, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the primary provisioning server.

39. An apparatus comprising:

means for operating a first provisioning system authorized to provision a processing device on a network, wherein the provisioning system is within a trusted environment; and

means for using the first provisioning system to authorize a second provisioning system outside the trusted environment to provision the processing device.

40. A method of operating a mobile device on a wireless network, the method comprising:

receiving a provisioning message from a first trusted provisioning domain (TPD), the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the mobile device;

storing information identifying the second TPD and the parameter in response to the provisioning message; and

provisioning the parameter in the mobile device in response to a provisioning message from the second TPD.

41. A method as recited in claim 40, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment.

42. A method as recited in claim 41, further comprising:

receiving a digital certificate of the second TPD from the first TPD; and

using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD.

43. A method as recited in claim 40, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, the method further comprising storing

information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.

44. A method of operating a mobile device on a wireless network, the method comprising:

receiving a provisioning message from a remote source, the provisioning message specifying a parameter;

determining whether the remote source is a primary trusted provisioning domain (TPD);

if the remote source is the primary TPD, provisioning the parameter in the mobile device in response to the provisioning message;

if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the mobile device from the primary TPD; and

if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the mobile device in response to the provisioning message.

45. A method as recited in claim 44, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment.

46. A method as recited in claim 44, further comprising:

receiving a digital certificate of the secondary TPD from the primary TPD; and

using the digital certificate in the mobile device to authenticate the provisioning message.

47. A method as recited in claim 44, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.

48. A mobile device configured to operate on a wireless network, the mobile device comprising:

a processor;

a data communication device coupled to the processor to communicate data with one or more remote systems via the wireless network; and

a memory coupled to the processor and storing instructions for execution by the processor to configure the mobile device to execute a process comprising

receiving a provisioning message from a first trusted provisioning domain (TPD) via the wireless network, the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the mobile device;

storing information identifying the second TPD and the parameter in response to the provisioning message; and

provisioning the parameter in the mobile device in response to a provisioning message from the second TPD.

49. A mobile device as recited in claim 48, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment.

50. A mobile device as recited in claim 49, wherein the process further comprises:

receiving a digital certificate of the second TPD from the first TPD; and

using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD.

51. A mobile device as recited in claim 48, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.

52. A mobile device configured to operate on a wireless network, the mobile device comprising:

a processor;

a data communication device coupled to the processor to communicate data with one or more remote systems via the wireless network; and

a memory coupled to the processor and storing instructions for execution by the processor to configure the mobile device to execute a process comprising

receiving a provisioning message from a remote source, the provisioning message specifying a parameter;

determining whether the remote source is a primary trusted provisioning domain (TPD);

if the remote source is the primary TPD, provisioning the parameter in the mobile device in response to the provisioning message;

if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the mobile device from the primary TPD; and

if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the mobile device in response to the provisioning message.

53. A mobile device as recited in claim 52, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment.

54. A mobile device as recited in claim 52, wherein the process further comprises:

receiving a digital certificate of the secondary TPD from the primary TPD; and

using the digital certificate in the mobile device to authenticate the provisioning message.

55. A mobile device as recited in claim 52, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.